

(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization International Bureau

(43) International Publication Date  
17 June 2004 (17.06.2004)

PCT

(10) International Publication Number  
WO 2004/051458 A2(51) International Patent Classification<sup>7</sup>: G06F 7/58(21) International Application Number:  
PCT/IB2003/005265(22) International Filing Date:  
18 November 2003 (18.11.2003)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:  
60/431,341 5 December 2002 (05.12.2002) US

(71) Applicant (for all designated States except US): KONINKLIJKE PHILIPS ELECTRONICS N.V. [NL/NL]; Groenewoudseweg 1, NL-5621 BA Eindhoven (NL).

(72) Inventors; and

(75) Inventors/Applicants (for US only): MITCHUM, Sam [US/US]; P.O. Box 3001, Briarcliff Manor, NY 10510-8001 (US). EHRHARDT, Jack [US/US]; P.O. Box 3001, Briarcliff Manor, NY 10510-8001 (US). LESTER, Bill [US/US]; P.O. Box 3001, Briarcliff Manor, NY 10510-8001 (US).

(74) Common Representative: KONINKLIJKE PHILIPS ELECTRONICS N.V.; c/o WAXLER, Aaron, P.O. Box 3001, Briarcliff Manor, NY 10510-8001 (US).

(81) Designated States (national): AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RU, SC, SD, SE, SG, SK, SL, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, YU, ZA, ZM, ZW.

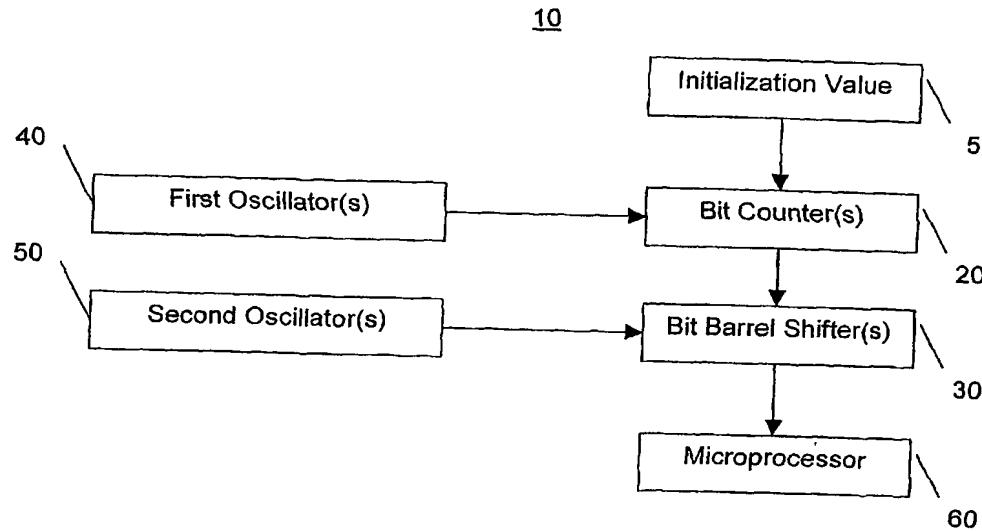
(84) Designated States (regional): ARIPO patent (BW, GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IT, LU, MC, NL, PT, RO, SE, SI, SK, TR), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

## Declaration under Rule 4.17:

— as to applicant's entitlement to apply for and be granted a patent (Rule 4.17(ii)) for all designations

[Continued on next page]

(54) Title: SYSTEM AND METHOD FOR TRUE RANDOM NUMBER GENERATION



WO 2004/051458 A2

(57) Abstract: There is provided a system and method for providing an entirely digital and/or digitally synthesizable true random number generator for incorporation on integrated circuits using any standard logic synthesis tool or comparable technique. The system and method has at least a microprocessor operating at a first frequency, at least one counter for generating bits, at least one shifter for scrambling bits, at least one first oscillator for cooperating with the at least one counter; and at least one second oscillator for cooperating with the at least one shifter. The system being configured to provide a frequency perturbation based on digital input signals initialized via the microprocessor.

W 2004/051458 A2



**Published:**

— without international search report and to be republished upon receipt of that report

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.